CHAPTER 15

INTELLIGENCE LAW

REFERENCES

1. National Security Act of 1947, 50 U.S.C. § 401-441d.
2. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801-1863.
3. Classified Information Procedures Act of 1980, 18 U.S.C. App.
4. Congressional Oversight Act, 50 U.S.C. § 413.
5. Executive Order 12333, United States Intelligence Activities, December 4, 1981, 46 F.R. 59941.
6. Executive Order 12863, President's Foreign Intelligence Advisory Board, September 13, 1993, 58 F.R. 48441.
7. DoD Dir. 5240.1, DoD Intelligence Activities, 25 April 1988
8. DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, 7 December 1982.
9. DoD Dir. 5240.2, DoD Counterintelligence, 22 May 1997.
10. AR 381-10, U.S. Army Intelligence Activities, 1 July 1984.
11. AFI 14-104, Oversight of Intelligence Activities, 1 Jul 2000.
12. AFI 90-201, Inspector General Activities, 26 Oct 2000.
13. SECNAVINST 3820.3D, Oversight Of Intelligence Activities With The Department Of The Navy, 26 August 1988.
14. AFI 71-101, Volume 1, Criminal Investigations, 1 December 1999.
15. SECNAVINST 3850.2B, Department Of The Navy Counterintelligence, 24 February 1991.
16. (S) AR 381-102, Intelligence Operational Support Activities (U).
17. (C) AR 381-141, Provisions for Administration, Supervision, Control and Use of Intelligence Contingency Funds (ICF) (U).
18. AFI 14-101, Intelligence Contingency Funds, 1 November 1998.
19. (C) AR 381-143, Intelligence Property (U).
20. (C) AR 715-30, Secured Environment Contracting (U).
21. (S) AR 381-172, Counterintelligence Force Protection Source Operations (CFSO) and Low Level Source Operations (LLSO) (U), 30 December 1994.
22. Defense HUMINT Service, Intelligence Law Handbook, September 1995.
23. Military Rules of Evidence, Rule 505.

Introduction. Intelligence is information. This information is essential to a commander in conducting operations and in accomplishing his mission. Rudimentary in its early origins, intelligence collection has become a sophisticated and essential operational discipline. Because intelligence is so important to the commander, operational lawyers must understand the basic tenets of Intelligence Law.

Intelligence in General. Intelligence can be either strategic or tactical. Strategic intelligence is that information necessary for the National Command Authority to make policy decisions in the realm of national security. Such intelligence is gathered from numerous collection methodologies such as human intelligence (HUMINT), electronics intelligence (ELINT), signals intelligence (SIGINT), or measures and signature intelligence (MASINT). This intelligence is normally nonperishable and is collected and analyzed for the consumer on a long term basis. Tactical intelligence is that intelligence which a commander uses to ascertain the capabilities of a threat. It is usually of a perishable and temporary nature.

Statutory Basis. In general, the statutory basis for Intelligence Law is found in:

1. The National Security Act of 1947, 50 U.S.C. §§ 401- 441d.

2. The Intelligence Oversight Act of 1980, 50 U.S.C. § 413.

3. Executive Order 12333, U.S. Intelligence Activities, Dec. 4 1981, 46 F.R. 59941.

4. Annual Intelligence Authorization Acts.

The Intelligence Community. The intelligence community is large and has a varied mission. The community is headed by the Director of Central Intelligence (DCI). The DCI is also the head of the Central Intelligence Agency (CIA). He is the President's principle legal advisor in all foreign and domestic intelligence matters.[1] The Department of Defense is supported by the Defense Intelligence Agency (DIA), the National Security Agency (NSA) and the various Service intelligence commands, such as the U.S. Army Intelligence and Security Command and its major subordinate units, including the various military intelligence brigades located throughout the world. In consultation with the DCI, the Secretary of Defense must implement policies and resource decisions of the DCI by DoD elements within the National Foreign Intelligence Program, while ensuring that the tactical intelligence activities provide responsive and timely support to operational commanders.[2]

Operational Issues. Aspects of intelligence law exist in all operations. It is imperative that operational lawyers consider them when planning and reviewing both operations in general and intelligence operations in particular. The JOPES format puts the intelligence annex of the OPLAN/CONPLAN at Annex B. (see the chapter on Military Decision Making Process and OPLANS of this Handbook, which includes the JOPES format and each Annex with every appendix listed). Annex B is the starting point for the judge advocate to participate in the intelligence aspects of operational development.

1. **Intelligence collection against U.S. persons**. The restrictions on collection of intelligence against U.S. persons stems from Executive Order 12333. That Order required all government agencies to implement guidance consistent with the Order. DoD has done so in DoDD 5240.1 and its accompanying Regulation, DoD 5240.1-R. Each Service has issued complementary guidance, though they are all based on the text of DoD 5240.1-R.

a. DoD 5240.1-R is the **sole authority** for intelligence components to collect, retain, and disseminate intelligence concerning U.S. persons. In other words, unless specific authorization to collect, retain, or disseminate information is found in the Regulation, it cannot be done.

b. There are two threshold questions which must first be addressed. The first is determining whether information has been "collected." Information is collected when it has been received, in intelligible form (as opposed to raw data), by an employee of an intelligence component in the course of his official duties. The second question is whether the information collected is about a "U.S. person." A "U.S. person" is defined as a citizen, permanent resident alien, U.S. corporation, or association substantially composed of any of the above groups. Unless there is evidence to the contrary, a person or organization within the U.S. is presumed to be a U.S. person; outside the U.S. the presumption is that they are not U.S. persons.

c. Once the threshold matters have been met, the analysis then turns to whether the information may be properly **collected**. Procedure 2 of DoD 5240.1-R governs this area. In short, the intelligence component must have a mission to collect the information, the information must be contained within one of 13 categories of information presented in the Procedure, and must be collected by the least intrusive means.

d. Once collected, the component should determine whether the information may be **retained** (Procedure 3). In short, if properly collected, it may be retained. If the information was incidentally collected (that is, collected without a Procedure 2 analysis), it may be retained if post-collection analysis indicates that it could have been properly collected. Information may be temporarily retained for up to 90 days solely for the purpose of determining its proper retainability.

e. **Dissemination** to other agencies is governed by Procedure 4. In general, the other agency must have a reasonable need for the information. However, if disseminating to another DoD intelligence component, that determination need not be made because that component will do its own Procedure 2 and 3 analysis.

[1] 50 U.S.C. § 403-3.

[2] 50 U.S.C. § 403-5.

2. **Special Collection Techniques**. DoD 5240.1-R goes on to treat special means of collecting intelligence in subsequent Procedures. These Procedures govern the permissible techniques, the permissible targets, and the appropriate official who may approve the collection. The judge advocate confronting any of these techniques must consult the detailed provisions of DoD 5240.1R.

a. Electronic Surveillance – Procedure 5.

b. Concealed Monitoring – Procedure 6.

c. Physical Searches – Procedure 7.

d. Searches and Examinations of Mail – Procedure 8.

e. Physical Surveillance – Procedure 9.

f. Undisclosed Participation in Organizations – Procedure 10.

3. Counterintelligence. Counterintelligence is information that is gathered or activities conducted to protect against espionage and other intelligence activities, as well as sabotage or assassination. Such intelligence activities are usually conducted on behalf of foreign powers, organizations, persons or international terrorists. Counterintelligence is concerned with identifying and counteracting that threat to our national security.

a. Within the United States, the FBI has primary responsibility for conducting counterintelligence and coordinating the counterintelligence efforts of all other U.S. government agencies.[3] Coordination with the FBI will be in accordance with the "Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation," between the Attorney General and the Secretary of Defense, April 5, 1979, as supplemented by later agreements.

b. Outside the United States, the CIA has primary responsibility for conducting counterintelligence and coordinating the counterintelligence efforts of all other U.S. government agencies.[4] Procedures for coordinating counterintelligence efforts are found in Director of Central Intelligence Directive 5/1 (DCID 5/1), "Espionage and Counterintelligence Activities Abroad," December 19, 1984.

c. DoD has primary responsibility for conducting military-related counterintelligence world-wide.[5] These activities are typically carried out by Service counterintelligence units. Coordination of effort with the FBI or CIA, as appropriate, is still essential.

4. **Counterintelligence Force Protection Source Operations**. A critical force protection tool available to any deploying commander overseas. The regulation, AR 381-172 (S), is classified. As always, a key aspect of this type of operation is coordination with the Chief of Station of the Country Team via the appropriate Unified Command.

5. **Cover and Cover Support** (AR 381-102) (S). A judge advocate should become familiar with the basics of cover. Cover severs the operator from the true purpose of the operation and/or the fact that the operator is associated with the U.S. government. There are four types of cover: natural, artificial, official and nonofficial. Considerations in the development of a cover plan are that the cover should be logical and normal for the operator, the operator must be able to live and fit the cover and the cover should be backstopped (a mechanism to defeat inquiries as to that cover). Remember, you can't make a silk purse out of a sow's ear! The National Security Act specifies that elements of the Intelligence Community may not use as an agent or asset for the purposes of collecting intelligence any individual who is authorized by contract or press credentials to represent themselves as a correspondent of a U.S. news media organization, or is officially recognized by a foreign government as a member of a U.S. media organization.[6] This prohibition can be waived

[3] EO 12333, ¶ 1.14(a).

[4] EO 12333, ¶ 1.8(c) and (d).

[5] EO 12333, ¶ 1.11(b).

[6] 50 U.S.C. § 403-7.

with a written determination by the President or DCI, and does not limit the voluntary cooperation of any person who is aware that they are assisting an element of the U.S. Intelligence Community.

6. **Support Issues Concerning Intelligence Operations.** The rules don't change regarding the support of intelligence operations. Money and property must be accounted for and goods and services still must be procured using appropriate federal acquisition regulations. The following classified regulations cover these important issues:

1. (U) Intelligence funding, *see* AR 381-141 (C).

2. (U) Intelligence property accountability, *see* AR 381-143 (C).

3. (U) Intelligence procurement, *see* AR 715-30 (C).

7. **Intelligence Oversight.** A critical aspect of all intelligence operations and activities is overseeing their proper execution, particularly when they relate to collection of intelligence against U.S. persons. A judge advocate may be called upon to advise an intelligence oversight officer of an intelligence unit or may be asked to be an intelligence oversight officer. EO 12333, the Intelligence Oversight Act (50 U.S.C. § 413) and DoD 5240.1-R, Procedure 15, provide the proper regulatory guidance regarding intelligence oversight.